

How to Secure a SCADA System without Replacement

by Lee Daniel

August 24, 2004

Insecure SCADA systems exist in industry and municipalities. In fact, there are so many that the Department of Homeland Security and the GAO consider this a critical problem and one with consequences as serious as any other threat facing this country. However, SCADA systems are not necessarily insecure because of some general design problem. Some companies have simply lessened security for the sake of convenience. This article will address common shortcomings of SCADA system access which, if addressed, would dramatically improve security without any need to upgrade or replace the existing SCADA system.

External Connection/Offsite Control

If external monitoring or control is not absolutely necessary, then do not allow it. The more physically disconnected from the outside a control system is, the less avenues there are available to exploit. However, sometimes an external connection is unavoidable such as power substations, or it is necessitated by a business model such as using an external company to operate a plant. Both of these exceptions are usually found in the public utility industry. For public utilities, there are many documents available on how to secure remote access points. Following these well defined published guidelines will lead to success.

The last typical exception to allowing a remote connection is the on-call engineer who needs to be able to check plant operation from his home. In this case, it is important that this connection not be allowed to control anything. It should only have the ability to view the current state of the process. For almost all cases, this is sufficient. If a control action needs to take place, then contact the on-site operator and let them make the change. The biggest advantage of a read-only connection is that even if it is compromised no one can use it to make an undesirable process change. If the technology currently being used to remotely "check on the process" can be used to make process changes, then this should be immediately reevaluated and replaced with a read-only technology. As with the public utilities, there are many vendor specific solutions available today. Not only are they available, but they can be very cheap. In fact, you are probably paying more to have the ability to change the process than you would to just view the process.

Local Area Network (LAN) and Wide Area Network (WAN) Connections

Many corporations make plant data available via a wide area network (WAN) or a Business to Business (BTB) connection. Additionally, this same data is available in a facility via a local area network (LAN). For most corporate users outside of the operator's room, they only need the data from the process historian, probably for reporting. However, most businesses allow corporate users to connect with write



permissions. So, they can not only report the data, they can change the data. This is true for data historian access and screen access such as PI Process Books or WonderWare (to name a couple). Why give them this kind of access by default? You are merely inviting trouble. The IT equivalent would be to give everyone administrative rights to the corporate network and assume that users will only do what you want them to do. In reality by making them administrators, they can do ANYTHING they want to. And as Murphy's Law would tell you, 'if it can happen, it will.' So, do not allow it to happen in the first place.

Sensors, and Logic Controllers

In today's plants, many sensors and Logic Controllers are directly on the facility LAN, sometimes wired and sometimes wirelessly. In most cases, the control network is not physically or logically separated from the general network. This in and of itself is inviting trouble. If it is not possible to physically separate the networks then at least logically separate them using network devices such as routers and firewalls. Not separating the control network leaves controllers and operators open to many types of attacks such as denial of service (DoS) and others. It also allows unauthorized users to directly access devices such as PLCs which is certainly not desirable.

There are some more intelligent sensors and logic controllers on the market. This equipment has features such as encryption and digital signing of control actions. You should use good password practices. As much of a pain as it might be to remember a different password for each controller, it's much more secure if you do. Not only should the passwords be different, but they should be changed at some regular interval. For wireless devices, it's especially important to use encryption and strong passwords. It is well documented that a "bad guy" can sit outside the perimeter of a facility and with a directional antenna (read Pringles can) and a laptop that person can access an unprotected wireless network. Digital signing is another great feature. Each control action is digitally signed and verified by the controller BEFORE the action is taken. This ensures that unauthorized signals to the controller are not acted upon.

Conclusion

While these recommended solutions are all standard in the IT world, they have not made their way into practice in the control system world. Vendors need to step up and explain why the precautions are needed and enforce these types of security techniques with their customers. If the vendors will not step up, then the Department of Homeland Security or some other government agency will have to mandate changes to industry. Security gaps are potentially just as costly as any problem that environmental laws regulate. So, this should be given equal importance and soon.